Chapter 14
Providing Security in Internet of Things Using Quantum Cryptography

Siva Sangari
Sathyabama Institute of Science and Technology, India

ABSTRACT

Quantum computing has gained an advantage in recent years due to its compatibility and usage in various fields. The IoT environment is huge, and almost the whole world relies on it to enable efficient data transmissions. Security of the internet of things is a major concern. This is because it deals with personal data, has to be reliable, and can direct and manipulate device decisions in a harmful way. When quantum computing is combined with IoT, the system's performance is drastically improved. Shor's algorithm is used to secure this proposed quantum computing system for IoT. Shor's algorithm is more secure than other existing algorithms.

INTRODUCTION

The evolution of Internet-of-Things (IoT) technology has served as the cornerstone for various industrial sectors, including agriculture, healthcare and logistics. The future-looking industry is guided on a path of maximum automation and efficiency development with IoT at its core. In actuality, it is anticipated that there will be close to 50 billion connected IoT devices worldwide by 2025. With such a high reliance on IoT, data accuracy analysis for this cutting-edge paradigm is essential. Lot of advanced development in quantum computing and implement quantum-resistant cryptographic algorithms advances traditional cryptography as a result of recent advances in the science of quantum computing. The accuracy and ideal behavior of data segments acquired by widely dispersed in IoT systems that are the focus of Data accuracy analysis. The prevalence of data mistakes, missing segments, and distorted perception renders the underlying IoT environment untrustworthy when several devices are embedded in the ambient environment to accomplish a common purpose. The main focus of the research presented is, obviously, on improving accuracy in a real-time IoT context by reducing sensor space. The two types of Data Ac-

DOI: 10.4018/978-1-6684-6697-1.ch014

curacy in the IoT sensor environment are different category those are tangible and intangible sensors. The Internet of Things (IoT) is problematically changing numerous areas of current life. Whether they are intended to make shrewd homes more agreeable, to work with clinical and medical care or to improve modern cycles in the Industrial IoT (IIoT), the quantity of uses that use IoT gadgets is developing broadly. Nonetheless, the IoT additionally bears various dangers, and security is viewed as quite possibly of its most basic issue, particularly since the number, exertion and capacities of vindictive assaults on IoT frameworks are filling with respect to the quantity of web associated gadgets. In this unique situation, the endeavor that was as of late found in the log4j-library has shown what weaknesses in generally utilized programming mean for some areas. Right now, data security is confronting one more danger in generally involved programming libraries because of the new advances in building Quantum PCs (QCs). The Shor Algorithm can be used to break several of the most widely used cryptosystems in use today. This approach efficiently resolves the existing problems in cryptographic algorithms. In its infancy, quantum computing is still restricted to a few mathematical operations that can be accurately predicted by related algorithms. We do need to create enough logical qubits that can be utilized to completely crack cryptographic algorithms. Quantum-resistant encryption methods need to be thoroughly tested utilizing ancient and modern data formats or sources in addition to all prior and ongoing advancements to make them interoperable with the supported platforms. And Modern public key algorithms are typically built around related issues. The tangible accuracy of IoT sensors is concerned with manufacturing flaws and the turnaround time between failure and repair. Sensor displacement, data acquisition time, and data sensing capacity in a chaotic environment are all issues with intangible correctness. The goal of the current study is to increase intangible accuracy in a real-time Internet of Things context. A dynamic challenge influenced by the traditional sensor placement problem is the minimization of IoT-sensor space. For this goal, a variety of optimization approaches have been used, but recent developments in quantum computing-inspired optimization (QCiO) have opened up new avenues for achieving optimal behavior. One of the most significant developments in calculations made in the 20th century is QCiO. In fact, this revolutionary idea has been studied by experts from all over the world to achieve the best outcomes in a variety of applications. Additionally, it is anticipated that the global market for quantum computing will surpass $1000 million by 2030.

RELATED WORK

Schöffel et.al(2022) similarly new KEMs and DSAs were deployed in such a representative architecture, and their effects on power usage, latency, and memory needs during TLS handshakes on an IoT edge device were evaluated. We learned the following novel insights as a result of our investigations. First, we demonstrate that rather than the cryptographic computation itself, the increased bandwidth demand of post-quantum primitives is the fundamental cause of the high TLS handshake time. Second, we show that, in contrast to NIST’s desire to standardize just one method, a clever mix of different DSAs produces the most energy-, latency-, and memory-efficient public key infrastructures. Third, we demonstrate that low-power IoT edge devices based on commercial Cortex M4 microcontrollers can implement code-based, isogeny-based, and lattice-based algorithms while maintaining functional battery life.

Abd El-Aziz et.al(2022) implemented the effects of these new KEMs and DSAs on the amount of memory, latency, and power used during TLS handshakes on an IoT edge device using such a representative architecture. We discovered the following novel findings as a result of our research. In the beginning,